**NASA TECHNICAL NOTE**

**NASA TN D-3863**

C.1



# CHARACTERIZATIONS OF REAL LINEAR ALGEBRAS

*by Anthony P. Cotroneo*

*Langley Research Center*
*Langley Station, Hampton, Va.*

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION • WASHINGTON, D. C. • FEBRUARY 1967

# CHARACTERIZATIONS OF REAL LINEAR ALGEBRAS

By Anthony P. Cotroneo

Langley Research Center
Langley Station, Hampton, Va.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

For sale by the Clearinghouse for Federal Scientific and Technical Information
Springfield, Virginia 22151 – CFSTI price $3.00

# CHARACTERIZATIONS OF REAL LINEAR ALGEBRAS*

By Anthony P. Cotroneo
Langley Research Center

## SUMMARY

Some characterizations and properties of linear algebras (or hypercomplex systems) over the field of real numbers are presented with essential definitions and theorems concerning real linear algebras on which neither the commutative property nor the associative property of multiplication is defined. Theorems relating the concepts of normed, absolute valued, and division algebras are also given.

In addition, algebras which are commutative or associative with respect to multiplication are considered. A construction of the algebra of real quaternions is given with a proof of the classical result of Frobenius which illustrates the unique place of complex numbers and quaternions among the algebras. Except for isomorphisms, the real numbers, the complex numbers, and the algebra of real quaternions form the only associative division algebras over the field of real numbers.

The algebra of real quaternions is discussed in detail. It is shown that all automorphisms on this algebra are of a specific type. These automorphisms form a group of linear orthogonal transformations which in turn define the group of all rotations on the real Euclidean vector space of dimension three. The technique of using quaternions to describe rigid-body rotations is especially useful in eliminating the singularities (gimbal lock) existing in the Euler angle rate equations. The illustrations presented point out many ways in which quaternions can be handled.

## INTRODUCTION

The study of linear algebras (or hypercomplex systems) began with W. R. Hamilton's discovery of quaternions. Hamilton was then primarily interested in the solution of two problems:

(1) Given an $n$ dimensional vector space, is it possible to define multiplication in such a way that the resultant system is a field?

---

*The information presented herein was submitted as a thesis in partial fulfillment of the requirements for the degree of Master of Arts, the College of William and Mary in Virginia, Williamsburg, Va., 1965.

(2) Can the product of two sums of n squares be expressed as a sum of n squares?

Hamilton defined a quaternion to be a quadruple of real numbers with the operations

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) + (\beta_1, \beta_2, \beta_3, \beta_4) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \alpha_3 + \beta_3, \alpha_4 + \beta_4)$$

and

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \cdot (\beta_1, \beta_2, \beta_3, \beta_4) = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$$

where

$$\gamma_1 = \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 - \alpha_4\beta_4$$
$$\gamma_2 = \alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_4 - \alpha_4\beta_3$$
$$\gamma_3 = \alpha_1\beta_3 - \alpha_2\beta_4 + \alpha_3\beta_1 + \alpha_4\beta_2$$
$$\gamma_4 = \alpha_1\beta_4 + \alpha_2\beta_3 - \alpha_3\beta_2 + \alpha_4\beta_1$$

He showed that all the axioms for a field were satisfied with the exception of the commutative law of multiplication. He was also able to obtain the striking identity

$$\left(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2\right) \cdot \left(\beta_1^2 + \beta_2^2 + \beta_3^2 + \beta_4^2\right) = \left(\gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_4^2\right)$$

Hamilton's discovery led to a great deal of interest and study in the areas of both linear algebra and applied mathematics. In mechanics, for example, quaternions have proved to be a useful tool in the representation of rigid-body rotations. Therefore, the algebra of real quaternions is treated in detail herein and should be particularly useful to individuals interested in the application of quaternions to describe rigid-body rotations.

The objective of this paper is to present some characterizations and properties of both nonassociative and associative linear algebras over the field of real numbers. Also included is a construction of the algebra of real quaternions from the system of complex numbers. By use of quaternions, one can construct still another but less attractive algebra, the eight dimensional Cayley algebra. Because defining this system is very involved, the system of Cayley numbers has not been presented in this paper. For a discussion of the properties and a proof of the uniqueness of this system, the reader is referred to references 1, 2, and 3.

Many of the theorems discussed in this report are treated in the various references. Because of the author's interest in the application of quaternions to rigid-body motion, this paper was written to present a logical and formal organization of pertinent material dealing with this subject.

## GENERAL CHARACTERIZATIONS

General characterization theorems of algebras over the field of real numbers are presented, with some definitions essential to the presentation.

Definition: Let A be a vector space of finite dimension n over the field R. Then A is a linear algebra of order n (or simply an algebra) if there is defined on A a product xy which satisfies the conditions

$$x(\alpha y) = (\alpha x)y = \alpha(xy) \qquad (\text{for } \alpha \text{ in } R \text{ and } x, y \text{ in } A)$$

$$\left.\begin{aligned} x(y + z) &= xy + xz \\ (y + z)x &= yx + zx \end{aligned}\right\} \qquad (\text{for } x, y, z \text{ in } A)$$

If R is the field of real numbers, A is called a real algebra. Also, if A contains an element $\epsilon$ such that $\epsilon x = x\epsilon = x$ for all x in A, A is said to be an algebra with identity and this element is denoted by "1." The definition does not assume commutativity or associativity of multiplication on the algebra A.

From this definition is derived the following useful representation of a product in A. Let $e_1, e_2, \ldots, e_n$ be a basis for A, and let

$$x = x_1e_1 + x_2e_2 + \ldots + x_ne_n$$

and

$$y = y_1e_1 + y_2e_2 + \ldots + y_ne_n$$

be any two elements in A. Then

$$xy = \sum_{i,j=1}^{n} x_iy_je_ie_j$$

is an element in A. Therefore,

$$e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k \qquad \left(i, j = 1, 2, \ldots, n; \ \gamma_{ijk} \text{ in } R\right)$$

so that

$$xy = \sum_{k=1}^{n} z_k e_k$$

$$z_k = \sum_{i,j=1}^{n} x_i y_j \gamma_{ijk} \qquad (k = 1, 2, \ldots, n)$$

Thus, multiplication of elements in A is completely determined by $n^3$ constants $\gamma_{ijk}$. These constants are called the structure constants of the system. Throughout this paper, R denotes the field of real numbers and it is understood that A is of finite dimension n. Also, to avoid confusion, in some instances a dot is used to indicate vector multiplication.

Definition: Let A be a real algebra; A is said to be absolute valued if there is a function $\phi$ on A to R such that

$$\phi(0) = 0$$

$$\phi(x) > 0 \qquad (\text{if } x \neq 0)$$

$$\phi(xy) = \phi(x)\ \phi(y)$$

$$\phi(x + y) \leqq \phi(x) + \phi(y)$$

and

$$\phi(\alpha x) = |\alpha| \phi(x)$$

for all x, y in A and $\alpha$ in R. If these properties hold, $\phi$ is designated an absolute value function on A. If $\phi(xy) \leqq \phi(x)\phi(y)$, A is said to be a normed algebra and $\phi$ is called a norm function on A.

Theorem 1: Every real algebra is a normed algebra.

Proof: Let A be a real algebra having a basis $e_1, e_2, \ldots, e_n$. Multiplication on A is defined by

$$e_i e_j = \sum_k \gamma_{ijk} e_k$$

where the $\gamma_{ijk}$'s are real. Now, let

$$u_i = \alpha e_i \qquad (i = 1, 2, \ldots, n)$$

for any nonzero real number $\alpha$. Then $u_1, u_2, \ldots, u_n$ forms a new basis for A such that

$$u_i u_j = \sum_k \delta_{ijk} u_k$$

and where $\delta_{ijk} = \alpha\gamma_{ijk}$. Let

$$x = \sum_i x_i u_i$$

and

$$y = \sum_j y_j u_j$$

be any two elements in A; then

$$xy = \sum_k z_k u_k$$

where

$$z_k = \sum_{i,j} x_i y_j \delta_{ijk}$$

Now choose $\alpha$ such that

$$\left|\delta_{ijk}\right| \leqq \frac{1}{n} \qquad (i, j, k = 1, 2, \ldots, n)$$

so that

$$\left|z_k\right| \leqq \frac{1}{n} \sum_{i,j} \left|x_i y_j\right|$$

Now define

$$\phi(w) = |w| = \left|w_1\right| + \left|w_2\right| + \ldots + \left|w_n\right|$$

for every

$$w = \sum_i w_i u_i$$

in A. Since

$$\phi(xy) = |xy| = \sum_k \left|z_k\right| \leqq \sum_{i,j} \left|x_i\right| \left|y_j\right| = |x|\,|y|$$

and

$$\phi(x + y) = |x + y| = \sum_i \left|x_i + y_i\right| \leqq |x| + |y|$$

$\phi$ is a norm function on A and clearly satisfies the remaining properties which must hold for a norm function. Hence A is a normed algebra and the proof is complete. This theorem is treated in reference 1.

Definition: A is a division algebra if the equations $ax = b$ and $ya = b$ always possess solutions for $a \neq 0$.

Theorem 2: Every real absolute valued algebra is a division algebra.

Proof: Let $A$ be a real algebra with absolute value function $\phi$. For some $a$ in $A$, define the mappings

$$xR_a = xa$$

$\left(\text{or } R_a : x \to xa\right)$ and

$$xL_a = ax$$

$\left(\text{or } L_a : x \to ax\right)$ for all $x$ in $A$. Then $R_a$ and $L_a$ are linear transformations on $A$. If $a \neq 0$ and $x \neq 0$, then $\phi(a) > 0$ and $\phi(x) > 0$ implies that $\phi(xa) > 0$ and hence $xa \neq 0$. Therefore, if $a \neq 0$, the null space of $R_a$ consists of the zero vector alone and similarly the null space of $L_a$ consists of the zero vector alone. Hence, if $a \neq 0$, $R_a$ and $L_a$ are nonsingular linear transformations on $A$. Thus, it follows that the equations $xa = b$ and $ax = b$ can be solved when $a \neq 0$. This theorem is discussed in references 1 and 4.

Definition: Let $A$ be an algebra and let $P$ and $Q$ be nonsingular linear transformations on $A$. The algebra $A^*$ whose elements are those of $A$ but whose product operation is defined by $x * y = xP \cdot yQ$ is called an isotope of $A$. Therefore, $A$ and $A^*$ are said to be isotopic.

Theorem 3: If $A$ is a real absolute valued algebra, then $A$ has an absolute valued isotope with identity. Furthermore, the absolute value function of $A$ is preserved in its isotope.

Proof: Let $\phi$ be an absolute value function defined on $A$. Since $\phi(\alpha x) = |\alpha| \phi(x)$ for every real $\alpha$ and $x$ in $A$, there exists a nonzero element $\epsilon$ in $A$ such that $\phi(\epsilon) = 1$. As before, since $\epsilon \neq 0$ and $A$ is absolute valued, $xR_\epsilon = x\epsilon$ and $xL_\epsilon = \epsilon x$ define nonsingular linear transformations on $A$. Let $x, z$ be any elements in $A$ such that

$$xR_\epsilon^{-1} = z$$

Then

$$x = zR_\epsilon = z\epsilon$$

and

$$\phi(x) = \phi\left(zR_\epsilon\right) = \phi(z) = \phi\left(xR_\epsilon^{-1}\right)$$

Similarly,

$$\phi(x) = \phi\left(xL_\epsilon^{-1}\right)$$

Now define an isotope $A^*$ of $A$ by

$$x * y = xR_\epsilon^{-1} \cdot yL_\epsilon^{-1}$$

Since $A$ and $A^*$ are the same linear spaces over $R$, the properties of $\phi$ involving addition and scalar multiplication are preserved on $A^*$. Also,

$$\phi(x * y) = \phi\left(xR_\epsilon^{-1}\right) \cdot \phi\left(yL_\epsilon^{-1}\right) = \phi(x)\phi(y)$$

for all $x, y$ in $A^*$. Therefore, $A^*$ is absolute valued and preserves the absolute value function of $A$.

Finally, consider the product $\epsilon^2 * y$ in $A^*$. The product of two linear transformations $R$ and $L$ is defined by

$$x(R \cdot L) = (xR) \cdot L$$

for all $x$ in $A$. Thus,

$$\epsilon^2 * y = \epsilon^2 R_\epsilon^{-1} \cdot yL_\epsilon^{-1} = \epsilon\left(yL_\epsilon^{-1}\right) = \left(yL_\epsilon^{-1}\right)L_\epsilon = y$$

for all $y$ in $A$. In a similar fashion

$$x * \epsilon^2 = x$$

for all $x$ in $A$. Hence, $\epsilon^2$ is the identity of $A^*$. Discussion of this theorem is given in reference 1.

Definition: Let $A$ be a real algebra with the basis $e_1, e_2, \ldots, e_n$. Denote the vector scalar product of

$$x = x_1e_1 + x_2e_2 + \ldots + x_ne_n$$

and

$$y = y_1e_1 + y_2e_2 + \ldots + y_ne_n$$

by $\langle x, y\rangle$. The norm of the vector $x$ is defined by

$$\langle x, x\rangle = N(x) = x_1^2 + x_2^2 + \ldots + x_n^2$$

In the theorems which follow, use is made of the fact that the scalar product defines a nondegenerate and symmetric bilinear form on $A$ – that is,

$$\langle x, A\rangle = 0 \quad \text{implies} \quad x = 0$$

$$\langle x, y\rangle = \langle y, x\rangle \quad \text{for all} \quad x, y \quad \text{in} \quad A$$

$$\left.\begin{aligned} \langle x, \alpha y + \beta z\rangle &= \alpha\langle x, y\rangle + \beta\langle y, z\rangle \\ \langle \alpha x + \beta y, z\rangle &= \alpha\langle x, z\rangle + \beta\langle y, z\rangle \end{aligned}\right\} \quad \text{for all real} \quad \alpha, \beta \quad \text{and all} \quad x, y, z \quad \text{in} \quad A$$

If $A$ is not associative, then $x^n$ is not uniquely defined in $A$. Therefore, in order to give meaning to $x^n$, define

$$x^n = x^{n-1} \cdot x \qquad (n = 2, 3, \ldots)$$

Lemma 1: Let $A$ be a real algebra such that $N(xy) = N(x)\,N(y)$ for all $x, y$ in $A$. If $x^n = x^{n-1} \cdot x$, where $n = 2, 3, \ldots$, then $N\left(x^k\right) = N(x)^k$ for all positive integers $k$.

Proof by induction: Let $x$ be any element in $A$. The lemma is obviously true for $k = 1$. Now let $k$ be an arbitrary positive integer such that

$$N\left(x^k\right) = N(x)^k$$

Then,

$$N\left(x^{k+1}\right) = N\left(x^k \cdot x\right) = N\left(x^k\right) N(x) = N(x)^k N(x) = N(x)^{k+1}$$

Hence,

$$N\left(x^k\right) = N(x)^k$$

for all positive integers $k$.

Theorem 4: Let A be a real algebra with identity. If $N(xy) = N(x)N(y)$ for all x, y in A, then A is absolute valued and the absolute value function defined on A is unique.

Proof: Define

$$\phi(x) = \|x\| = +\sqrt{N(x)}$$

for all x in A. Then

$$\phi(x + y) = \|x + y\| = +\sqrt{\langle x + y, x + y\rangle}$$

so that

$$\|x + y\|^2 \leqq \|x\|^2 + 2|\langle x, y\rangle| + \|y\|^2$$

By use of the Cauchy-Schwarz inequality,

$$\|x + y\|^2 \leqq \|x\|^2 + 2\|x\|\,\|y\| + \|y\|^2 = \left(\|x\| + \|y\|\right)^2$$

and, hence,

$$\phi(x + y) = \|x + y\| \leqq \|x\| + \|y\| = \phi(x) + \phi(y)$$

The remaining properties which must hold for $\phi$ to be an absolute value function are clearly satisfied and thus A is absolute valued.

To avoid confusion between the identity in A and the identity in R, the identity in A is denoted by $\epsilon$. Let $\epsilon, e_2, e_3, \ldots, e_n$ form a basis for A. If $\phi$ is an absolute value function on A, then

$$\phi(\epsilon) = \phi(\epsilon\epsilon) = \phi(\epsilon)\phi(\epsilon)$$

and, hence,

$$\phi(\epsilon) = 1$$

Now suppose $\phi(x)$ is not unique on A. Then there exists an absolute value function $\theta(x)$ on A such that $\theta(a) \neq \phi(a)$ for some $a \neq 0$ in A. Therefore, either $\theta(a) > \phi(a)$ or $\theta(a) < \phi(a)$.

Consider first $\theta(a) > \phi(a)$. If

$$y = \frac{a}{\|a\|}$$

then

$$\|y\| = +\sqrt{N(y)} = 1$$

Let

$$y^k = y_1\epsilon + y_2e_2 + \ldots + y_ne_n$$

Also

$$\theta(y) > 1 \quad \text{since} \quad \theta(y) = \frac{\theta(a)}{\|a\|} > \frac{\phi(a)}{\|a\|} = 1$$

Furthermore, by lemma 1,

$$1 = N\left(y^k\right) = {y_1}^2 + {y_2}^2 + \ldots + {y_n}^2$$

which implies $|y_i| \leqq 1$. Since $\theta$ is an absolute value function,

$$\theta(y)^k = \theta\left(y^k\right) \leqq |y_1|\ \theta(\epsilon) + |y_2|\ \theta\left(e_2\right) + \ldots + |y_n|\ \theta\left(e_n\right)$$

and, hence,

$$\theta(y)^k \leqq 1 + \theta\left(e_2\right) + \ldots + \theta\left(e_n\right)$$

But this is impossible since $\theta(y) > 1$ and $k$ is arbitrary.

Now consider $\theta(a) < \phi(a)$. Since $A$ is absolute valued, it is a division algebra. Therefore, the equation $az = \epsilon$ can be solved whenever $a \neq 0$. Let $y = \|a\|z$; then

$$\theta(y) = \|a\|\theta(z)$$

But since

$$\theta(a)\ \theta(z) = \theta(\epsilon) = 1$$

then

$$\theta(y) = \frac{\| a \|}{\theta(a)} > \frac{\| a \|}{\phi(a)} = 1$$

and

$$\phi(y) = 1$$

The rest of the proof for $\theta(a) < \phi(a)$ proceeds exactly as that for $\theta(a) > \phi(a)$ – that is, a contradiction is arrived at to the assumption that $\theta(a) < \phi(a)$. Hence $\theta(x) = \phi(x)$ for all $x$ in $A$, so that $\phi(x)$ is unique.

Lemma 2: Let $A$ be a real algebra such that $N(xy) = N(x)\,N(y)$ for all $x, y$ in $A$; then for all $x, y$ and $x', y'$ in $A$

(1) $\langle xy, x'y\rangle = \langle x, x'\rangle N(y)$

and

$\langle xy, xy'\rangle = N(x)\langle y, y'\rangle$

(2) $\langle xy, x'y'\rangle + \langle xy', x'y\rangle = 2\langle x, x'\rangle\langle y, y'\rangle$

Proof: It can easily be established that for all $x, y$ in $A$

$$\langle x, y\rangle = \frac{1}{2}\Big[N(x + y) - N(x) - N(y)\Big]$$

Then

$$\langle xy, x'y\rangle = \frac{1}{2}\Big[N(xy + x'y) - N(xy) - N(x'y)\Big] = \langle x, x'\rangle N(y)$$

Similarly,

$$\langle xy, xy'\rangle = N(x)\langle y, y'\rangle$$

Therefore,

$$\langle x(y + y'), x'(y + y')\rangle = \langle x, x'\rangle N(y + y')$$

However,

$$N(y + y') = 2\langle y, y'\rangle + N(y) + N(y')$$

Hence

$$\langle x(y+y'), x'(y+y')\rangle = 2\langle x, x'\rangle\langle y, y'\rangle + \langle x, x'\rangle N(y) + \langle x, x'\rangle N(y')$$

$$= 2\langle x, x'\rangle\langle y, y'\rangle + \langle xy, x'y\rangle + \langle xy', x'y'\rangle$$

Now since

$$\langle x(y+y'), x'(y+y')\rangle = \langle xy, x'y\rangle + \langle xy, x'y'\rangle + \langle xy', x'y\rangle + \langle xy', x'y'\rangle$$

then

$$\langle xy, x'y'\rangle + \langle xy', x'y\rangle = 2\langle x, x'\rangle\langle y, y'\rangle$$

This lemma is treated in references 4 and 5 and is used in the proof of the next characterization theorem.

Definition: Let $A$ and $B$ be algebras over a field $F$. A one-to-one mapping $\psi$ of $A$ onto $B$ is called an isomorphism of $A$ onto $B$ if the operations of addition and multiplication are preserved under the mapping – that is,

$$\psi(\alpha a + \beta b) = \alpha\psi(a) + \beta\psi(b)$$

$$\psi(ab) = \psi(a)\,\psi(b)$$

for all $a, b$ in $A$ and $\alpha, \beta$ in $F$. Algebras $A$ and $B$ are said to be isomorphic if there exists an isomorphism of $A$ onto $B$. By an automorphism of an algebra $A$ is meant an isomorphism of $A$ onto itself. If a mapping $\psi$ is an isomorphism (or automorphism) except that

$$\psi(ab) = \psi(b)\,\psi(a)$$

$\psi$ is said to be an anti-isomorphism (or anti-automorphism).

Definition: An algebra $A$ is termed an alternative algebra if for every $x, y$ in $A$, $x^2y = x(xy)$ and $xy^2 = (xy)y$.

Theorem 5: Let $A$ be a real algebra with identity 1. If $N(xy) = N(x)N(y)$ for all $x, y$ in $A$, then $A$ is an alternative algebra with involution (anti-automorphism) $\psi : x \to \bar{x}$ such that

$$x\bar{x} = N(x)\cdot 1$$

and

$$x + \bar{x} = T(x)\cdot 1 \qquad (T(x) \text{ is real})$$

Proof: Let $I$ denote the subspace of $A$ spanned by the identity and let $I^{\perp}$ denote its orthogonal complement. Then $A$ is a direct sum of $I$ and $I^{\perp}$ and is written $A = I \oplus I^{\perp}$ – that is, every $x$ in $A$ can be written as $\alpha\cdot 1 + a$ for some real $\alpha$ and $a$ in $I^{\perp}$. For a proof of this the reader is referred to reference 6, page 157.

For $x = \alpha\cdot 1 + a$ in $A$, define $\bar{x} = \alpha\cdot 1 - a$ and consider the mapping $\psi : x \to \bar{x}$ given by $\psi(x) = \bar{x}$. Clearly

$$\psi(\alpha x + \beta y) = \alpha\psi(x) + \beta\psi(y)$$

It is now shown that

$$\psi(xy) = \psi(y)\,\psi(x)$$

If $x' = 1$ and $x$ is taken in $I^{\perp}$, then by (2) of lemma 2

$$\langle xy, y'\rangle + \langle xy', y\rangle = 2\langle x, 1\rangle\langle y, y'\rangle = 0$$

for all $y, y'$ in $A$. Also, by the law of multiplication defined on $A$,

$$\langle(\alpha\cdot 1)y, y'\rangle - \langle y, (\alpha\cdot 1)y'\rangle = 0$$

for all real $\alpha$. Thus,

$$\langle xy, y'\rangle + \langle(\alpha\cdot 1)y, y'\rangle + \langle xy', y\rangle - \langle(\alpha\cdot 1)y', y\rangle = 0$$

and

$$\langle(x + \alpha\cdot 1)y, y'\rangle = \langle(\alpha\cdot 1 - x)y', y\rangle$$

for all real $\alpha$, $x$ in $I^{\perp}$ and $y, y'$ in $A$. Now, if $w = \alpha\cdot 1 + x$, then $\langle wy, y'\rangle = \langle y, \bar{w}y'\rangle$ for all $w, y, y'$ in $A$. Similarly, if $y' = 1$ and $y$ is in $I^{\perp}$ in (2) of lemma 2, $\langle xz, x'\rangle = \langle x, x'\bar{z}\rangle$ for all $x, x', z$ in $A$. Combining these results gives, for all $x, y, z$ in $A$,

$$\langle xy, z\rangle = \langle y, \bar{x}z\rangle = \langle y\bar{z}, \bar{x}\rangle = \langle \bar{z}, \bar{y}\bar{x}\rangle$$

If $x = 1$, then $\langle y, z\rangle = \langle \bar{z}, \bar{y}\rangle$. Therefore

$$\langle xy, z\rangle = \langle \bar{z}, \bar{x}\bar{y}\rangle$$

Thus,

$$\langle \bar{z}, \bar{y}\bar{x}\rangle - \langle \bar{z}, \bar{x}\bar{y}\rangle = 0$$

which implies that $\bar{y}\bar{x} = \bar{x}\bar{y}$ and

$$\psi(xy) = \bar{x}\bar{y} = \bar{y}\bar{x} = \psi(y)\,\psi(x)$$

Now suppose that $\psi(x) = \psi(y)$ for some $x, y$ in $A$. Then, since $\psi(\bar{x}) = x$,

$$x = \psi(\psi(x)) = \psi(\psi(y)) = y$$

Since $\psi$ is an onto mapping, it defines an involution on $A$.

The subspace $I$ contains all those elements of $A$ left fixed by the involution and $I^{\perp}$ contains all $x$ in $A$ such that $\psi(x) = -x$. Since $\psi(x\bar{x}) = x\bar{x}$, then $x\bar{x}$ is in $I$, so there exists a real number $\alpha$ such that $x\bar{x} = \alpha\cdot 1$. Now,

$$\alpha = \alpha\langle 1, 1\rangle = \langle \alpha\cdot 1, 1\rangle = \langle x\bar{x}, 1\rangle = \langle (1\cdot x), x\rangle = N(x)$$

Hence $x\bar{x} = N(x)\cdot 1$ for all $x$ in $A$. Also,

$$x\bar{x} = N(\bar{x})\cdot 1 = N(x)\cdot 1$$

Finally, since $x + \bar{x}$ is left fixed by $\psi$, there is a real number $\beta$ such that $x + \bar{x} = \beta\cdot 1$. Now $x + \bar{x} = T(x)\cdot 1$, where $T(x)$ is a linear functional and is defined to be the trace of $x$.

To complete the proof, it remains to show that the alternative law is satisfied for all elements in $A$. From the first part of this proof $\langle xy, xz\rangle = \langle y, \bar{x}(xz)\rangle$ for all $x, y, z$ in $A$. But $\langle xy, xz\rangle = N(x)\langle y, z\rangle$ from (1) of lemma 2. Hence,

$$\langle y, \bar{x}(xz)\rangle - \langle y, N(x)\cdot z\rangle = \langle y, \bar{x}(xz) - (x\bar{x})z\rangle = 0$$

This implies that $\bar{x}(xz) = (x\bar{x})z$. Since there exists some real number $\beta$ such that $x + \bar{x} = \beta \cdot 1$, then

$$\bar{x}(xz) = (\beta \cdot 1 - x)(xz) = (\beta \cdot 1)(xz) - x(xz)$$

and

$$(x\bar{x})z = \left[x(\beta \cdot 1 - x)\right] z = (\beta \cdot 1)(xz) - x^2 z$$

Hence

$$x(xz) = x^2 z$$

for all $x, z$ in $A$. If $\langle xz, yz \rangle$ is considered, it can similarly be shown that

$$xz^2 = (xz)z$$

for all $x, z$ in $A$. Thus $A$ is alternative and the proof is complete. This theorem is discussed in references 4 and 5.

A direct consequence of this theorem is the following corollary.

Corollary: Let $A$ be a real algebra with identity $1$ and let $I$ denote the subspace spanned by the identity of $A$. If $N(xy) = N(x)N(y)$ for all $x, y$ in $A$, then every element of $A$ satisfies the quadratic equation $x^2 - T(x) \cdot x + N(x) \cdot 1 = 0$ over $I$. Furthermore, the space $I$ is the set of all elements left fixed by the involution $\psi(x) = \bar{x}$, whereas $I^{\perp}$ is the set of all $a$ in $A$ such that $\psi(a) = \bar{a} = -a$.

The proof of the converse to this theorem depends on the validity of the Moufang identity on an alternative algebra – that is,

$$(xy)(zx) = x\left[(yz)x\right]$$

for all $x, y, z$ in $A$. In view of this, lemma 3 is presented and is of value in proving the converse to this theorem. Denote the set of all n-tuples of elements in $A$ by $A^n$ and make the following definitions:

Definition: The associator of an algebra $A$ is a function $S$ defined on $A^3$ to $A$ by

$$S(x, y, z) = (xy)z - x(yz)$$

for all $x, y, z$ in $A$.

Definition: Let $A$ be an arbitrary algebra and let $f(x_1, x_2, \ldots, x_n)$ be a multilinear function defined on $A^n$ to $A$. The function $f$ is said to be skew-symmetric provided (1) $f$ takes on the value $0$ whenever at least two of its arguments are equal, and (2) $f$ changes sign whenever two of its arguments are interchanged.

Lemma 3: Let $A$ be an alternative algebra over a field $F$ and define the function $K$ from $A^4$ to $A$ by

$$K(w, x, y, z) = S(wx, y, z) - xS(w, y, z) - S(x, y, z)\cdot w$$

for all $w, x, y, z$ in $A$; then $S$ and $K$ are linear skew-symmetric functions.

Proof: The proof is contained in two parts.

I. That $S$ is linear in $x$ is readily verified by expanding $S(\alpha x_1 + \beta x_2, y, z)$ for any $x_1, x_2, y, z$ in $A$ and $\alpha, \beta$ in $F$. Similarly $S$ is linear in $y$ and $z$. It is also clear that $S(x, x, y) = 0 = S(x, y, y)$ when $A$ is an alternative algebra. Therefore,

$$S(x, y + z, y + z) = S(x, y, z) + S(x, z, y) = 0$$

and

$$S(y + z, y + z, x) = S(z, y, x) + S(y, z, x) = 0$$

Thus

$$S(x, y, z) = -S(x, z, y) \quad \text{and} \quad S(z, y, x) = -S(y, z, x)$$

Finally,

$$S(x, y, z) = -S(x, z, y) = S(z, x, y) = -S(z, y, x)$$

Hence $S$ is a linear skew-symmetric function from $A^3$ to $A$.

II. Now consider the function $K$. It is immediate that $K$ is linear from the linearity of $S$. Also, from the definition of $K$, note that $K(w, x, y, y) = 0$. Therefore,

$$K(w, x, y, z) = -K(w, x, z, y)$$

since

$$K(w, x, y + z, y + z) = K(w, x, y, z) + K(w, x, z, y) = 0$$

A function $G$ on $A^4$ is now defined by

$$G(w, x, y, z) = S(wx, y, z) - S(w, xy, z) + S(w, x, yz) - wS(x, y, z) - S(w, x, y)\cdot z$$

By expanding all the associators it is found that $G(w, x, y, z) = 0$ and, therefore,

$$-K(z, w, x, y) = G(w, x, y, z) - K(z, w, x, y)$$

Expanding $G$ and $K$ in terms of their associators and applying part I of this lemma gives

$$-K(z, w, x, y) = S(wx, y, z) - S(xy, z, w) + S(yz, w, x) - S(zw, x, y)$$

By use of

$$S(wx, y, z) = K(w, x, y, z) + xS(w, y, z) + S(x, y, z)\cdot w$$

it is found that a cyclic permutation of the elements $z, w, x, y$ changes the sign on the right-hand side of the expression for $-K(z, w, x, y)$ – that is,

$$K(y, z, w, x) = -K(z, w, x, y)$$

Thus, for all $w, x, y, z$ in $A$,

$$K(w, x, y, z) = -K(w, x, z, y)$$

and

$$K(w, x, y, z) = -K(z, w, x, y)$$

Since these two permutations of the elements $w, x, y, z$ generate the entire symmetric group of permutations, the skew-symmetry of $K$ has been proved. This lemma is treated in references 3 and 7.

Lemma 3 is now used to prove the converse to theorem 5.

Converse: Let $A$ be a real algebra with identity 1. If $A$ is an alternative algebra with involution $\psi : x \to \bar{x}$, where $x\bar{x} = N(x)\cdot 1$ and $x + \bar{x} = T(x)\cdot 1$ ($T(x)$ is a real number), then $N(xy) = N(x)N(y)$ for all $x, y$ in $A$.

Proof: First prove the validity of the Moufang identity on $A$. It can be easily verified that

$$(xy)(zx) = x\left[y(zx)\right] + S(x, y, zx)$$

From lemma 3,

$$S(x, y, zx) = -S(zx, y, x) = -S(x, y, x)\cdot z - xS(z, y, x) - K(z, x, y, x)$$

and, therefore,

$$S(x, y, zx) = xS(y, z, x) = x\left[(yz)x\right] - x\left[y(zx)\right]$$

Hence

$$(xy)(zx) = x\left[(yz)x\right]$$

for all $x, y, z$ in $A$. Since $x + \bar{x} = T(x)\cdot 1$ for all $x$ in $A$, then

$$x^2y + (x\bar{x})y = \left[x(T(x)\cdot 1)\right]y$$

and

$$x(xy) + x(\bar{x}y) = x\left[(T(x)\cdot 1)y\right]$$

for all $x, y$ in $A$. By the law of multiplication defined on $A$,

$$\left[x(T(x)\cdot 1)\right]y = T(x)\cdot(xy) = x\left[(T(x)\cdot 1)y\right]$$

Therefore, since $A$ is an alternative algebra,

$$(x\bar{x})y = x(\bar{x}y)$$

Similarly,

$$x(y\bar{y}) = (xy)\bar{y}$$

For every x, y in A,

$$N(xy)\cdot 1 = (xy)(\bar{y}\bar{x}) = (xy)\left[\bar{y}(T(x)\cdot 1 - x)\right]$$
$$= T(x)\cdot(xy)\bar{y} - (xy)(\bar{y}x)$$

By the Moufang identity

$$N(xy)\cdot 1 = T(x)\left[x(y\bar{y})\right] - x\left[(y\bar{y})x\right]$$
$$= T(x)\,N(y)\cdot x - N(y)\cdot x^2$$

and, hence,

$$N(xy)\cdot 1 = N(y)\cdot x\left[T(x)\cdot 1 - x\right] = N(y)\cdot(x\bar{x}) = N(y)\,N(x)\cdot 1$$

The converse to theorem 5 is discussed in references 4 and 5.

## COMMUTATIVE AND ASSOCIATIVE ALGEBRAS

In the previous section the assumption of commutativity and associativity of multiplication concerning real linear algebras was ignored. In this section further characterizations and uniqueness of real linear algebras having these properties are presented.

Definition: A skew field is a ring in which the nonzero elements form a group under multiplication. A commutative skew field is called a field.

Theorem 6: Let A be a real division algebra. If multiplication on A is associative, then A is a skew field. (If, in addition, A is commutative with respect to multiplication, then A is a field.)

Proof: If A is associative with respect to multiplication, then A is a ring. Let a, b be nonzero elements of A. Since A is a division algebra, there is an element x in A such that $ax = b$. Similarly, there is an element y in A such that $by = x$. Hence $a(by) = ax = b$. Since $b \neq 0$ and $a(by) = (ab)y$, it follows that $ab \neq 0$. Thus A has no nonzero divisors of zero. It can now be shown that A has an identity.

Let a be any nonzero element in A. There exists an element $\epsilon$ in A such that $a\epsilon = a$. Then $\epsilon \neq 0$. Now $a\epsilon^2 = a\epsilon$, which implies that $\epsilon^2 = \epsilon$ since a is not a divisor of zero. Let x be any element in A. Then

$$(x - x\epsilon)\epsilon = 0$$

and

$$\epsilon(x - \epsilon x) = 0$$

Hence $x\epsilon = \epsilon x = x$, so that $\epsilon$ is the identity element of A. As before, this element is denoted by 1.

It is now shown that every nonzero element of A has a multiplicative inverse. Let a be any nonzero element of A. There exists an x in A such that $ax = 1$. Then $x \neq 0$. Furthermore,

$$(xa - 1)x = x(ax) - x = 0$$

Therefore, $xa - 1 = 0$ or $xa = 1$ and, hence, x is the inverse of a. It has been shown that the nonzero elements of A form a multiplicative group. Hence A is a skew field. Furthermore, if A is commutative with respect to multiplication, then A is a commutative skew field or simply a field. This theorem is treated in reference 8, pages 18-21.

It shall now be proved that except for isomorphisms, the real and complex numbers form the only commutative division algebras over the real numbers. As before, the space spanned by the identity of A is denoted by I. Since A is real, I is clearly isomorphic to the field of real numbers.

Definition: An element a in A is said to be in the center of A if $ax = xa$ for all x in A.

Definition: Let A be a division algebra with identity 1 over a field F. A is said to be algebraic over a field K if (1) K is contained in the center of A, and (2) every element a in A satisfies a nontrivial polynomial with coefficients in K.

In this and following theorems the center of A is denoted by C(A).

Lemma 4: If A is a real associative division algebra, then A is algebraic over I. Furthermore, each element of A satisfies a nontrivial linear or quadratic equation over I.

Proof: Since A is an associative division algebra, A has an identity; since A is real, I is isomorphic to the field of real numbers. Also, if $\alpha$ is any real number, then by the rule of multiplication defined on A, $(\alpha \cdot 1)a = a(\alpha \cdot 1)$ for all a in A. Thus I is contained in C(A).

Since A is associative, the product of k factors a can be expressed by $a^k$. If A is of order n, the set of $n + 1$ elements (that is, $1, a, a^2, \ldots, a^n$) are linearly dependent with respect to R. Hence there exist real numbers $\alpha_0, \alpha_1, \ldots, \alpha_n$, not all zero, such that

$$\alpha_0 \cdot 1 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0$$

Therefore a is a root of an equation of degree $\leqq n$ with coefficients in I. If

$$p(x) = \alpha_0 \cdot 1 + \alpha_1 x + \ldots + \alpha_n x^n$$

and since I is isomorphic to R, by the fundamental theorem of algebra

$$p(x) = f_1(x) \cdot f_2(x) \ldots f_k(x)$$

$k \leqq n$, and $f_i(x)$ is of degree 1 or 2. Since $p(a) = 0$, some $f_i(a) = 0$ and thus a is a root of a linear or quadratic equation over I. This lemma is discussed in reference 9, page 10.

Lemma 5: Let A be an associative division algebra over the field C of complex numbers. If A is algebraic over $C^* = C \cdot 1$, then $A = C^*$.

Proof: Since A is algebraic over $C^*$ and if a is any element of A, there exist complex numbers $c_0, c_1, c_2, \ldots, c_n$, not all zero, such that

$$c_0 \cdot 1 + c_1 a + \ldots + c_n a^n = 0$$

Again, by making use of the fundamental theorem of algebra, the polynomial

$$p(x) = c_0 \cdot 1 + c_1 x + \ldots + c_n x^n$$

can be factored into a product of linear factors – that is,

$$p(x) = \left(x - \lambda_1 \cdot 1\right)\left(x - \lambda_2 \cdot 1\right)\left(x - \lambda_3 \cdot 1\right) \ldots \left(x - \lambda_n \cdot 1\right)$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are in C. Now since $p(a) = 0$, some

$$a - \lambda_i \cdot 1 = 0$$

Hence a is in $C^*$ and it has been shown that $A \subseteq C^*$. Since A is algebraic over $C^*$, $C^* \subseteq A$. Therefore, $A = C^*$. This lemma is treated in reference 6, pages 326-327.

Theorem 7: Let $A$ be a real associative division algebra. If $A$ is commutative, then $A$ is isomorphic to either the field of real numbers or the field of complex numbers.

Proof: By lemma 4, $A$ is algebraic over $I$ and hence $I$, which is isomorphic to $R$, is contained in $C(A)$. Suppose that $I \neq A$; then there exists an $a$ in $A$ which is not in $I$. Therefore, $a$ satisfies some quadratic equation with real coefficients. Otherwise, $a$ would be in $I$. Let

$$p(x) = x^2 + 2\alpha x + \alpha_0 \cdot 1$$

such that $p(a) = 0$ and where $\alpha$ and $\alpha_0$ are real. Then

$$(a + \alpha \cdot 1)^2 = \alpha^2 \cdot 1 - \alpha_0 \cdot 1$$

For any $x$ in $A$ and $\gamma'$ in $R$, if $x^2 = \gamma' \cdot 1$ and $\gamma' > 0$, there is a real number $\gamma$ such that

$$x^2 = \gamma^2 \cdot 1$$

Then

$$x^2 - \gamma^2 \cdot 1 = (x + \gamma \cdot 1)(x - \gamma \cdot 1) = 0$$

which implies that $x = \pm\gamma \cdot 1$. Hence $\alpha^2 - \alpha_0 < 0$ for if this were positive, there would exist a $\gamma$ in $R$ such that

$$a + \alpha \cdot 1 = \pm\gamma \cdot 1$$

However, this implies that $a$ is in $I$. Hence, there is a real number $\beta$ such that $\alpha^2 - \alpha_0 = -\beta^2$. Therefore

$$(a + \alpha \cdot 1)^2 = -\beta^2 \cdot 1$$

Thus, if $a$ is in $A$ but not in $I$, real numbers $\alpha, \beta$ can be found such that

$$\left(\frac{a + \alpha \cdot 1}{\beta}\right)^2 = -1$$

Set

$$i = \left(\frac{a + \alpha \cdot 1}{\beta}\right)$$

so that $i^2 = -1$ and, hence, A contains $I + I \cdot i$ which is isomorphic to the field of complex numbers. This field is denoted by $C^*$. It remains only to show that $A = C^*$.

Since A is algebraic over I, then A is algebraic over $C^*$. If a in A satisfies a polynomial with coefficients in I, then a clearly satisfies a polynomial with coefficients in $C^*$. Also, $C^* \subseteq C(A)$ since A is commutative. Therefore, by lemma 5, $C^* = A$ and the proof is complete. This theorem is treated in reference 6, page 327.

The property of commutativity on A is now dropped and the characterization of real division algebras which are associative is continued.

Theorem 8: Let A be an associative division algebra. For some a contained in A, let $R_a$ and $L_a$ be the linear transformations on A such that $xR_a = xa$ and $xL_a = ax$ for all x in A. Then A is isomorphic to

$$A_R = \left\{R_x \mid x \text{ in } A\right\}$$

and anti-isomorphic to

$$A_L = \left\{L_x \mid x \text{ in } A\right\}$$

Proof: Define $\psi(x) = R_x$ for all x in A and show that $\psi$ defines an isomorphism of A onto $A_R$. First consider

$$\psi(\alpha x + \beta y) = R_{\alpha x + \beta y}$$

for x, y in A and $\alpha$, $\beta$ in R. Note that for any a in A

$$aR_{\alpha x+\beta y} = a(\alpha x + \beta y) = \alpha\left(aR_x\right) + \beta\left(aR_y\right)$$

Hence

$$R_{\alpha x+\beta y} = \alpha R_x + \beta R_y$$

so that

$$\psi(\alpha x + \beta y) = \alpha\psi(x) + \beta\psi(y)$$

Now consider $\psi(xy) = R_{xy}$. For $a$ in $A$,

$$aR_{xy} = a(xy) = (ax)y = \left(aR_x\right)R_y = a\left(R_x \cdot R_y\right)$$

Hence

$$R_{xy} = R_x R_y$$

so that

$$\psi(xy) = \psi(x)\,\psi(y)$$

Finally, suppose $\psi(x) = \psi(y)$ and let $a$ be any nonzero element in $A$. Then $aR_x = aR_y$ so that $a(x - y) = 0$ and, since $A$ is an associative division algebra, $x = y$. Therefore, since $\psi$ is an onto mapping, $A$ is isomorphic to $A_R$.

Now consider the mapping $\psi'(x) = L_x$. Note that for $a$ in $A$,

$$aL_{xy} = (xy)a = x(ya) = \left(aL_y\right)L_x = a\left(L_y \cdot L_x\right)$$

Hence

$$\psi'(xy) = \psi'(y)\,\psi'(x)$$

so that $\psi'$ defines an anti-isomorphism from $A$ onto $A_L$.

Thus, if $A$ is an associative division algebra with basis $e_1, e_2, \ldots, e_n$ and if

$$x = x_1e_1 + x_2e_2 + \ldots + x_ne_n$$

is any element in $A$, then

$$x \longrightarrow x_1R_{e_1} + x_2R_{e_2} + \ldots + x_nR_{e_n}$$

under the mapping $\psi$ and

$$x \longrightarrow x_1 L_{e_1} + x_2 L_{e_2} + \ldots + x_n L_{e_n}$$

under the mapping $\psi'$. Therefore, $R_{e_1}, R_{e_2}, \ldots, R_{e_n}$ form a basis for $A_R$ and $L_{e_1}, L_{e_2}, \ldots, L_{e_n}$ form a basis for $A_L$. This theorem is treated in reference 10. pages 240-241.

Theorem 9: Let $A$ be a real associative division algebra; then the algebras $A_R$ and $A_L$ of linear transformations on $A$ are isomorphic to algebras of real $n \times n$ matrices.

Proof: Let

$$x = x_1 e_1 + x_2 e_2 + \ldots + x_n e_n$$

where $x_i$ is real and $e_1, e_2, \ldots, e_n$ form a basis for $A$. Now $xR_a = xa$ is in $A$ so that

$$xR_a = xa = y = y_1 e_1 + y_2 e_2 + \ldots + y_n e_n$$

$$y = \left(\sum_i x_i e_i\right) R_a = \sum_i x_i \left(e_i R_a\right)$$

and

$$e_i R_a = \sum_j \alpha_{ij} e_j$$

Now

$$y = xR_a = \sum_i x_i \sum_j \alpha_{ij} e_j = \sum_j \left(\sum_i \alpha_{ij} x_i\right) e_j$$

and, hence,

$$y_j = \sum \alpha_{ij} x_i$$

with the matrix $\left(\alpha_{ij}\right)$ denoted by $m\left(R_a\right)$. Thus, the linear transformation $R_a$ which sends the vector $x$ having components $(x_1, x_2, \ldots, x_n)$ into the vector $y$ having components $(y_1, y_2, \ldots, y_n)$ can be represented by the real $n \times n$ matrix $(\alpha_{ij})$ where $e_i R_a = \sum_j \alpha_{ij} e_j$.

The mapping $\theta(R_x) = m(R_x)$ for all $x$ in $A$ is now shown to define an isomorphism of $A_R$ onto $M(A_R) = \{m(R_x) \mid R_x \text{ in } A_R\}$.

First, note that for real $\alpha, \beta$ and $R_x, R_y$, in $A_R$

$$\theta(\alpha R_x + \beta R_y) = m(\alpha R_x + \beta R_y) = \alpha m(R_x) + \beta m(R_y)$$

since

$$e_i(\alpha R_x + \beta R_y) = \alpha(e_i R_x) + \beta(e_i R_y)$$

Suppose

$$e_i R_x = \sum_j \alpha_{ij} e_j$$

and

$$e_j R_y = \sum_k \beta_{jk} e_k$$

then

$$e_i(R_x R_y) = \sum_j \alpha_{ij}(e_j R_y) = \sum_j \alpha_{ij} \sum_k \beta_{jk} e_k$$

Therefore,

$$e_i(R_x R_y) = \sum_{j,k} \alpha_{ij} \beta_{jk} e_k$$

which implies that

$$m(R_x R_y) = (\alpha_{ij})(\beta_{jk}) = m(R_x) \cdot m(R_y)$$

that is,

$$m\left(R_x R_y\right) = \left(\tau_{ik}\right) = \sum_j \alpha_{ij}\beta_{jk}$$

Hence

$$\theta\left(R_x R_y\right) = m\left(R_x\right) m\left(R_y\right)$$

Now suppose $\theta\left(R_x\right) = \theta\left(R_y\right)$; then $m\left(R_x - R_y\right) = (0)$. If

$$m\left(R_x - R_y\right) = \left(\alpha_{ij}\right)$$

each $\alpha_{ij} = 0$ so that

$$e_i\left(R_x - R_y\right) = e_i(x - y) = 0$$

which implies that $x = y$ so that $R_x = R_y$. Hence the mapping $\theta$ is an isomorphism of $A_R$ onto $M\left(A_R\right)$.

Similarly, if

$$M\left(A_L\right) = \left\{m\left(L_x\right) \mid L_x \text{ in } A_L\right\}$$

it can be shown that the mapping $\theta'$ defined by

$$\theta'\left(L_x\right) = m\left(L_x\right)$$

for all $x$ in $A$ is an isomorphism of $A_L$ onto $M\left(A_L\right)$. This subject is discussed in reference 10, pages 202-213.

Corollary: Let $A$ be a real associative division algebra; then $A$ is isomorphic to the algebra $M\left(A_R\right)$ and anti-isomorphic to the algebra $M\left(A_L\right)$.

Definition: The isomorphism $A \cong M\left(A_R\right)$ is known as the first regular representation of $A$ and the anti-isomorphism $A \cong M\left(A_L\right)$ is called the second regular representation of $A$.

Hence, given an associative division algebra $A$ with basis $e_1, e_2, \ldots, e_n$, there is for any

$$x = x_1 e_1 + x_2 e_2 + \ldots + x_n e_n$$

in A the following correspondence:

$$x \longleftrightarrow x_1 R_{e_1} + x_2 R_{e_2} + \ldots + x_n R_{e_n}$$

and

$$x \longleftrightarrow x_1 m\left(R_{e_1}\right) + x_2 m\left(R_{e_2}\right) + \ldots + x_n m\left(R_{e_n}\right)$$

Similarly

$$x \longleftrightarrow L_x \longleftrightarrow m\left(L_x\right)$$

An example of a regular representation of the algebra of complex numbers is as follows: Let C denote the algebra of complex numbers. Then 1, i is a basis for C, so that for any $\alpha + \beta i$ in C

$$\alpha + \beta i \longleftrightarrow \alpha R_1 + \beta R_i \longleftrightarrow \alpha\, m\left(R_1\right) + \beta\, m\left(R_i\right)$$

where $m\left(R_1\right)$ is given by

$$1R_1 = 1 + 0i$$

$$iR_1 = 0 + i$$

and $m\left(R_i\right)$ is given by

$$1R_i = 0 + i$$

$$iR_i = -1 + 0i$$

Therefore,

$$\alpha + \beta i \longleftrightarrow \alpha\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \beta\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}$$

Since C is a commutative algebra, the first and second regular representations of C are identical.

The algebra of real quaternions is constructed by imitating the construction of the complex numbers. Again, let C denote the algebra of complex numbers.

Consider the set Q of all ordered pairs (a, b) where a, b are complex numbers. For all complex numbers a, b, c, d the operation of addition on Q is defined by $(a, b) + (c, d) = (a + c, b + d)$. Scalar multiplication is given by $c(a, b) = (ca, cb)$. Under the given operations, Q is a vector space over the field of complex numbers. Each (a, b) in Q can be expressed as

$$(a, b) = a(1, 0) + b(0, 1)$$

Multiplication on Q is defined as follows:

$$(a, b)(c, d) = (ac - \bar{d}b, da + b\bar{c})$$

where the bar indicates the complex conjugate. The multiplicative identity is clearly $1 = (1, 0)$. If $j = (0, 1)$, then $j^2 = -1$. Now, every (a, b) in Q is uniquely expressible in the form

$$(a, b) = a\cdot 1 + bj$$

and the rule of multiplication on Q can be written as

$$(a\cdot 1 + bj)(c\cdot 1 + dj) = \left(ac - \bar{d}b\right)\cdot 1 + (da + b\bar{c})j$$

Let $a = \alpha_0 + \alpha_1\sqrt{-1}$ and $b = \alpha_2 + \alpha_3\sqrt{-1}$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are real; then,

$$(a, b) = a\cdot 1 + bj = \alpha_0\cdot 1 + \alpha_1\sqrt{-1}\cdot 1 + \alpha_2 j + \alpha_3\sqrt{-1}j$$

Let $\left(\sqrt{-1}, 0\right) = i$ and $\left(0, \sqrt{-1}\right) = k$. Thus, each element (a, b) in Q is uniquely represented in the form

$$(a, b) = \alpha_0\cdot 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

By this rule of multiplication is computed the following table which also defines multiplication on Q:

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k$$

$$jk = -ki = i$$

$$ki = -ik = j$$

Under this rule of multiplication,

$$Q = \left\{ \alpha_0 \cdot 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k \;\middle|\; \alpha_0, \alpha_1, \alpha_2, \alpha_3 \text{ real} \right\}$$

is a real associative algebra with identity. The elements of $Q$ are known as quaternions and $Q$ is called the algebra of real quaternions.

Theorem 10: The algebra of real quaternions is an absolute valued algebra.

Proof: Apply the converse to theorem 5. First, for every $q$ in $Q$ define the quaternion conjugate of $q$ by

$$\bar{q} = \alpha_0 \cdot 1 - \left(\alpha_1 i + \alpha_2 j + \alpha_3 k\right)$$

By simple multiplication it can easily be shown that the mapping $\psi(q) = \bar{q}$ defines an involution on $Q$. Similarly, it can be shown that $q\bar{q} = N(q) \cdot 1$ for all $q$ in $Q$. Finally, define $T(q) \cdot 1 = q + \bar{q}$ for all $q$; then $T(q)$ is clearly real. Since $Q$ is associative, $N(pq) = N(p)\,N(q)$ and the proof is complete.

This section is concluded with the following proof of the uniqueness of the algebra of real quaternions.

Theorem 11: Let $A$ be a real associative division algebra. If $A$ is not commutative, then $A$ is isomorphic to the algebra of quaternions.

Proof: It is first shown that $I = C(A)$. By lemma 4, $I \subseteq C(A)$. Suppose there exists an element $a$ in $C(A)$ such that $a$ is not in $I$. Then, as previously shown, there would exist real numbers $\alpha$, $\beta$ such that $\left(\frac{a + \alpha \cdot 1}{\beta}\right)^2 = -1$. Thus, $C(A)$ would contain a field $C^*$ isomorphic to the field of complex numbers. Hence, $A$ would be algebraic over $C^*$ and therefore by lemma 5, $A = C^*$. This contradicts the assumption that $A$ is not commutative. Therefore, $I = C(A)$.

Let $a$ be any element of $A$ such that $a$ is not in $I$ and take $i = \left(\frac{a + \alpha \cdot 1}{\beta}\right)$ such that $i^2 = -1$. Then $i$ is not in $I$ so there exists an element $b$ in $A$ such that

$$c = bi - ib \neq 0$$

Note that

$$ic + ci = i(bi - ib) + (bi - ib)i = ibi - i^2 b + bi^2 - ibi = 0$$

so that $ic = -ci$. Furthermore,

$$ic^2 = (ic)c = -(ci)c = c(ci) = c^2 i$$

so that $c^2$ commutes with $i$.

Now $c$ satisfies some quadratic equation over $I$. Let

$$c^2 + \gamma c + \delta \cdot 1 = 0 \qquad (\gamma, \delta \text{ real})$$

Since

$$\gamma c = -c^2 - \delta \cdot 1$$

then $\gamma c$ commutes with $i$. Hence

$$\gamma ci = i\gamma c = \gamma ic = -\gamma ci$$

and $2\gamma ci = 0$. Since $2ci \neq 0$ and $A$ is a division algebra, $\gamma = 0$. Therefore $c^2 = -\delta \cdot 1$. Also $c$ cannot be in $I$ since $ic = -ci$. Hence $\delta > 0$ so that $\delta = \xi^2$ ($\xi$ real).

Let $j = \frac{c}{\xi}$; then $j^2 = -1$. Also,

$$ji + ij = \frac{ci + ic}{\xi} = 0$$

and, therefore, $ij = -ji$. Let $k = ij$.

Hence $A$ contains the algebra $C^* + C^* \cdot j$ which is isomorphic to the algebra of real quaternions. This algebra is denoted by $Q^*$.

Finally it is shown that $Q^* = A$. Suppose $Q^* \neq A$. Then for some $x$ in $A$ but not in $Q^*$, an element $l$ can be determined in $A$ which is not in $Q^*$ and such that $l^2 = -1$. Now $i \pm l$ are roots of quadratic equations over $I$. For real $\alpha_1, \alpha_2, \beta_1, \beta_2$, let

$$(i + l)^2 + \alpha_1(i + l) + \alpha_2 \cdot 1 = 0$$

and

$$(i - l)^2 + \beta_1(i - l) + \beta_2 \cdot 1 = 0$$

Hence

$$(i + l)^2 = -2\cdot 1 + il + li = -\alpha_1(i + l) - \alpha_2\cdot 1$$

and

$$(i - l)^2 = -2\cdot 1 - il - li = -\beta_1(i - l) - \beta_2\cdot 1$$

Adding gives

$$\left(\alpha_1 + \beta_1\right)i + \left(\alpha_1 - \beta_1\right)l + \left(\alpha_2 + \beta_2 - 4\right)\cdot 1 = 0$$

Since $1, i, l$ are linearly independent,

$$\alpha_1 = \beta_1 = 0$$

and, therefore,

$$il + li = \alpha\cdot 1 \qquad (\alpha \ \text{real})$$

Similarly,

$$jl + lj = \beta\cdot 1$$

and

$$kl + lk = \gamma\cdot 1 \qquad (\beta, \gamma \ \text{real})$$

Thus

$$lk = (li)j = (\alpha\cdot 1 - il)j = \alpha j - i(\beta\cdot 1 - jl) = \alpha j - \beta i + kl$$

Then

$$2kl = \gamma\cdot 1 + \beta i - \alpha j$$

Multiplying by $k$ gives

$$-2l = \gamma k + \beta j + \alpha i$$

This result implies that $l$ is in $Q^*$ and contradicts the assumption that $Q^* \neq A$. Hence $A = Q^*$ and the proof is completed. This theorem is treated in reference 6, pages 327-329, and in reference 4, pages 100-112.

From some of the previous results the following corollary can be stated.

Corollary: Let A be a real associative absolute valued algebra. Then A is isomorphic to the real numbers, to the complex numbers, or to the real quaternions.

## THE ALGEBRA OF REAL QUATERNIONS

Let Q denote the algebra of real quaternions.

Theorem 12: Let p be a fixed nonzero quaternion. Then $\theta(q) = pqp^{-1}$ is an automorphism on Q. Furthermore, every automorphism on Q is of this type.

Proof: Since Q is an associative division algebra, every nonzero element of Q has a unique inverse. Consider

$$\theta(q) = pqp^{-1}$$

for all q in Q and some fixed nonzero element p. If $q_1$, $q_2$ are arbitrary elements in Q and $\alpha, \beta$ are real, then

$$\theta\left(\alpha q_1 + \beta q_2\right) = p\left(\alpha q_1 + \beta q_2\right)p^{-1} = \alpha p q_1 p^{-1} + \beta p q_2 p^{-1}$$

and, hence,

$$\theta\left(\alpha q_1 + \beta q_2\right) = \alpha\theta\left(q_1\right) + \beta\theta\left(q_2\right)$$

Also

$$\theta\left(q_1 q_2\right) = pq_1\left(p^{-1}p\right)q_2 p^{-1} = \left(pq_1p^{-1}\right)\left(pq_2p^{-1}\right)$$

so that

$$\theta\left(q_1 q_2\right) = \theta\left(q_1\right)\cdot\theta\left(q_2\right)$$

Finally, if $\theta\left(q_1\right) = \theta\left(q_2\right)$, then $q_1 = q_2$ since Q does not have any nonzero divisors of zero. Since $\theta$ is an onto mapping, $\theta$ is an inner automorphism on Q.

Now suppose $\theta'$ is an automorphism of Q and let

$$\theta'(q) = q'$$

Suppose that under the mapping $\theta'$

$$1 \longleftrightarrow 1$$

$$i \longleftrightarrow e_1$$

$$j \longleftrightarrow e_2$$

$$k \longleftrightarrow e_3$$

then $1, e_1, e_2, e_3$ obey the same rule of multiplication as defined for $1, i, j, k$. There now exist elements $p_1, p_2, p_3$ in Q such that

$$p_1 = e_3 j - e_2 k + e_1 + i$$

$$p_2 = e_1 k - e_3 i + e_2 + j$$

$$p_3 = e_2 i - e_1 j + e_3 + k$$

It is now shown that for every q in Q

$$q' p_1 = p_1 q$$

$$q' p_2 = p_2 q$$

and

$$q' p_3 = p_3 q$$

where $q'$ is the image of q under the mapping $\theta'$. By using the previously described rule of multiplication on Q,

$$e_1 p_1 = -e_2 j - e_3 k - 1 + e_1 i$$

and

$$p_1 i = -e_3 k - e_2 j + e_1 i - 1$$

so that

$$e_1p_1 = p_1i$$

Similarly,

$$e_2p_1 = p_1j$$

and

$$e_3p_1 = p_1k$$

Hence for every $q$ in $Q$,

$$q'p_1 = p_1q$$

and, similarly,

$$q'p_2 = p_2q$$

and

$$q'p_3 = p_3q$$

If one of the elements $p_1$, $p_2$, $p_3$ is not zero, the proof of the theorem is complete.

Now, suppose that

$$p_1 = p_2 = 0$$

then

$$e_1 + i = e_2k - e_3j$$

Also

$$p_2 = e_1k - e_3i + e_3e_1 - ik = e_3(e_1 - i) + (e_1 - i)k = 0$$

since

$$k^{-1} = \bar{k}/N(k) = -k$$

then

$$(e_1 - i) = e_3(e_1 - i)k = e_2k + e_3j$$

From

$$e_1 + i = e_2k - e_3j$$

is obtained

$$i = -e_3j$$

which implies that $e_3 = k$. Similarly, if

$$p_2 = p_3 = 0$$

then

$$i = e_1$$

and if

$$p_3 = p_1 = 0$$

then

$$j = e_2$$

Thus, if $p_1 = p_2 = p_3 = 0$, then $\theta'$ must be the identity mapping and $p = 1$. This completes the proof of the theorem. This theorem is discussed in reference 11, pages 257-259.

Theorem 13: The collection of all automorphisms on Q form a multiplicative group of linear orthogonal transformations on Q.

Proof: Let $G$ be the collection of all automorphisms on $Q$. By theorem 12, the elements of $G$ are linear transformations of the form $T_p$ where $p$ is a fixed nonzero quaternion and

$$qT_p = pqp^{-1}$$

for all $q$ in $Q$. First, note that $G$ is closed under multiplication – that is, suppose $p_1, p_2$ are fixed nonzero elements of $Q$; then for any $q$ in $Q$

$$q\left(T_{p_1} \cdot T_{p_2}\right) = \left(qT_{p_1}\right)T_{p_2} = (p_2p_1)q\left(p_1{}^{-1}p_2{}^{-1}\right)$$

But

$$p_1{}^{-1}p_2{}^{-1} = \bar{p}_1\bar{p}_2 / N(p_1p_2) = \bar{p}_2\bar{p}_1 / N(p_1p_2) = (p_2p_1)^{-1}$$

and, hence,

$$T_{p_1}T_{p_2} = T_{p_2p_1}$$

so that $G$ is closed. Similarly,

$$qT_{p_1}\left[\left(T_{p_2} \cdot T_{p_3}\right)\right] = q\left[\left(T_{p_1} \cdot T_{p_2}\right)T_{p_3}\right]$$

for fixed nonzero elements $p_1, p_2, p_3$ and $q$ in $Q$. Thus $G$ is associative.

Now, $T_1$ is clearly in $G$. If $T_p$ is any element of $G$ and $q$ is an arbitrary element of $Q$, then

$$q\left(T_1 \cdot T_p\right) = qT_p$$

and, therefore, $T_1$ is the identity in $G$. Finally, since each element of $G$ is a nonlinear transformation on $Q$, $T_p{}^{-1}$ exists for each $T_p$ in $G$. Hence $G$ is a multiplicative group of linear transformations on $Q$.

Note that for all $q$ in $Q$ and each $T_p$ in $G$,

$$\left\langle qT_p, qT_p\right\rangle = N\left(pqp^{-1}\right) = N(q) = \langle q, q\rangle$$

Thus $G$ is a group of linear orthogonal transformations on $Q$.

As for theorem 5, note that

$$Q = I \oplus I^{\perp}$$

where $I$ is isomorphic to the field of real numbers. Furthermore, from the construction of $Q$, $I^{\perp}$ is isomorphic to the real Euclidean vector space of dimension three. Denote $I^{\perp}$ by $E_3$. Then every element in $Q$ is of the form

$$q = r + v$$

where $r$ is in $I$ and $v$ in $E_3$.

Theorem 14: Let $G$ be the group of all automorphisms on $Q$. Then (1) the elements of $I$ are invariant under the transformations of $G$ and (2) $G$ defines the group of all rotations on $E_3$.

Proof: That the elements of $G$ leave the elements of $I$ fixed is clear since each $r$ in $I$ is of the form $\alpha \cdot 1$, where $\alpha$ is real. Thus, for each $r$ in $I$ and $T_p$ in $G$,

$$rT_p = p(\alpha \cdot 1)p^{-1} = r$$

and, hence, for any $q = r + v$ in $Q$ and $T_p$ in $G$,

$$qT_p = r + pvp^{-1}$$

Consider the effect of an element in $G$ on an element of $E_3$. Let

$$p = \alpha_0 \cdot 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

be any fixed nonzero element of $Q$, and let

$$v = xi + yj + zk$$

be an arbitrary element of $E_3$. Then

$$vT_p = pvp^{-1} = \frac{1}{N(p)}\left[pv\bar{p}\right]$$

Expanding this expression shows that $vT_p$ is in $E_3$. Since $T_p$ is an orthogonal transformation, $T_p$ defines either a rotation on $E_3$ or a rotation followed by a reflection on $E_3$. Let

$$v' = x'i + y'j + z'k$$

denote the vector in $E_3$ such that

$$vT_p = v'$$

From the expansion of $vT_p$ results the following matrix representation of this transformation:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \frac{1}{N(p)} \begin{bmatrix} \left(\alpha_0^2 + \alpha_1^2 - \alpha_2^2 - \alpha_3^2\right) & 2\left(\alpha_1\alpha_2 - \alpha_0\alpha_3\right) & 2\left(\alpha_1\alpha_3 + \alpha_0\alpha_2\right) \\ 2\left(\alpha_2\alpha_1 + \alpha_3\alpha_0\right) & \left(\alpha_0^2 + \alpha_2^2 - \alpha_3^2 - \alpha_1^2\right) & 2\left(\alpha_2\alpha_3 - \alpha_0\alpha_1\right) \\ 2\left(\alpha_3\alpha_1 - \alpha_2\alpha_0\right) & 2\left(\alpha_2\alpha_3 + \alpha_0\alpha_1\right) & \left(\alpha_0^2 + \alpha_3^2 - \alpha_1^2 - \alpha_2^2\right) \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = m\left(T_p\right) \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

Let $m\left(T_p\right)$ denote the matrix of the transformation $T_p$ and let

$$A(p) = N(p) \cdot m\left(T_p\right)$$

Since the determinant of $m\left(T_p\right)$ is given by

$$\det\left[m\left(T_p\right)\right] = \pm 1$$

then

$$\det A(p) = \pm N(p)^3$$

Inasmuch as $\det A(p)$ is a polynomial in $\alpha_0, \alpha_1, \alpha_2, \alpha_3$, it is a continuous function from

$$\left\{R^4 - (0, 0, 0, 0)\right\}$$

to R and is either always positive or always negative. That is, suppose there exist fixed nonzero quaternions $p_1$ and $p_2$ such that

$$\det A(p_1) > 0$$

and

$$\det A(p_2) < 0$$

Since

$$\left\{R^4 - (0, 0, 0, 0)\right\}$$

is connected, it is shown by the intermediate value theorem (ref. 12, p. 322) that there exists a $p_3$ in Q such that

$$\det A(p_3) = \pm N(p_3)^3 = 0$$

But this expression implies that $p_3 = 0$ which is impossible since $p_3 = 0$ is not in the domain of $\det A(p)$. Therefore,

$$\det\left[m\left(T_p\right)\right] = 1$$

for all $T_p$ in G or

$$\det\left[m\left(T_p\right)\right] = -1$$

for all $T_p$ in G. Now consider $T_{p'}$ in G defined by

$$p' = \alpha \cdot 1$$

Then clearly $\det A(p') = \alpha^6 = +N(p')^3$ and is positive for all transformations in G. Therefore,

$$\det\left[m\left(T_p\right)\right] = +1$$

for all $T_p$ in G. Hence G is a group of rotations on $E_3$.

It is now shown that G is the group of all rotations on $E_3$. Let R denote any rotation on $E_3$. From analytic geometry R can be defined by the direction cosines of the axis of rotation together with the angle of rotation about that axis. Let $\xi$, $\eta$, and $\zeta$ denote the direction cosines of the axis of rotation with the X, Y, and Z axes, respectively. Also, let $\omega$ denote the angle of rotation. Whittaker (ref. 13, p. 7) has shown that R has the following matrix representation:

$$\begin{bmatrix} 1 - 2\left(1 - \xi^2\right)\sin^2\frac{\omega}{2} & 2 \sin\frac{\omega}{2}\left(\xi\eta \sin\frac{\omega}{2} + \zeta \cos\frac{\omega}{2}\right) & 2 \sin\frac{\omega}{2}\left(\xi\zeta \sin\frac{\omega}{2} - \eta \cos\frac{\omega}{2}\right) \\ 2 \sin\frac{\omega}{2}\left(\xi\eta \sin\frac{\omega}{2} - \zeta \cos\frac{\omega}{2}\right) & 1 - 2\left(1 - \eta^2\right)\sin^2\frac{\omega}{2} & 2 \sin\frac{\omega}{2}\left(\eta\zeta \sin\frac{\omega}{2} + \xi \cos\frac{\omega}{2}\right) \\ 2 \sin\frac{\omega}{2}\left(\xi\zeta \sin\frac{\omega}{2} + \eta \cos\frac{\omega}{2}\right) & 2 \sin\frac{\omega}{2}\left(\eta\zeta \sin\frac{\omega}{2} - \xi \cos\frac{\omega}{2}\right) & 1 - \left(1 - \zeta^2\right)\sin^2\frac{\omega}{2} \end{bmatrix}$$

This matrix is precisely the matrix obtained when

$$\alpha_0 = \cos\frac{\omega}{2}$$

$$\alpha_1 = -\xi \sin\frac{\omega}{2}$$

$$\alpha_2 = -\eta \sin\frac{\omega}{2}$$

and

$$\alpha_3 = -\zeta \sin\frac{\omega}{2}$$

are substituted in the expansion of $vT_p = pvp^{-1}$ previously given. Now $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ cannot all be zero since

$$\xi^2 + \eta^2 + \zeta^2 = 1$$

Thus, a fixed nonzero quaternion is found – namely,

$$p = \cos\frac{\omega}{2}\cdot 1 - \xi \sin\frac{\omega}{2} i - \eta \sin\frac{\omega}{2} j - \zeta \sin\frac{\omega}{2} k$$

such that

$$vT_p = vR$$

Hence R is in G and the proof of the theorem is complete.

Corollary: The most general rotation of a vector $v$ in $E_3$ can be defined by

$$vT_p = pvp^{-1}$$

where

$$p = \cos\frac{\omega}{2}\cdot 1 - \sin\frac{\omega}{2}(\xi i + \eta j + \zeta k)$$

$\xi$, $\eta$, and $\zeta$ are the direction cosines of the axis of rotation with the $X$, $Y$, and $Z$ axes, respectively, and $\omega$ is the angle of rotation about the axis.

## CHARACTERIZATIONS OF QUATERNIONS

Some of the properties and characterizations of $Q$ which follow from the theorems of this paper are now given.

(1) Multiplication on $Q$ in Gibbs notation (see ref. 14, pp. 403-429): Let $[v_1, v_2]$ denote the vector cross product of elements in $E_3$. Then by the rule of multiplication defined on $Q$, it can readily be established that

(a) $$v_1v_2 = -\langle v_1, v_2\rangle\cdot 1 + [v_1, v_2]$$

Hence, for all $q_1 = r_1 + v_1$ and $q_2 = r_2 + v_2$,

(b) $$q_1q_2 = \left(r_1r_2 - \langle v_1, v_2\rangle\cdot 1\right) + \left(r_1v_2 + r_2v_1 + [v_1, v_2]\right)$$

The relationships (a) and (b) yield the following interesting identities:

(c) $$v_1v_2 + v_2v_1 = -2\langle v_1, v_2\rangle\cdot 1$$

$$v_1v_2 - v_2v_1 = 2[v_1, v_2]$$

$$v_1q_2 - q_2v_1 = 2[v_1, v_2]$$

and

$$q_1q_2 - q_2q_1 = 2[v_1, v_2]$$

(2) By theorem 10, $\psi(q) = \overline{q} = r - v$ is an involution on Q for all $q = r + v$ in Q, $\overline{q}$ being defined as the conjugate of q. Thus,

$$T(q)\cdot 1 = q + \overline{q} = 2r$$

$$N(q)\cdot 1 = q\overline{q} = \overline{q}q$$

$$\overline{\alpha p + \beta p} = \alpha\overline{p} + \beta\overline{q}$$

and

$$\overline{pq} = \overline{q}\,\overline{p}$$

for all p, q in Q and real $\alpha, \beta$.

(3) First regular representation of Q: Let

$$q = \alpha_0 \cdot 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

For some p in Q the linear transformation $R_p$ is defined by

$$qR_p = qp$$

for all q in Q. Then from theorems 8 and 9

$$q \longleftrightarrow \alpha_0 R_1 + \alpha_1 R_i + \alpha_2 R_j + \alpha_3 R_k$$

and

$$q \longleftrightarrow \alpha_0 m\left(R_1\right) + \alpha_1 m\left(R_i\right) + \alpha_2 m\left(R_j\right) + \alpha_3 m\left(R_k\right)$$

As an example, $m\left(R_i\right)$ is given by

$$1R_i = i = 0\cdot 1 + i + 0\cdot j + 0\cdot k$$

$$iR_i = i^2 = -1 + 0\cdot i + 0\cdot j + 0\cdot k$$

$$jR_i = ji = 0\cdot 1 + 0\cdot i + 0\cdot j - k$$

$$kR_i = ki = 0\cdot 1 + 0\cdot 1 + j + 0\cdot k$$

Thus,

$$m(R_1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$m(R_i) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$m(R_j) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

$$m(R_k) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

and, hence,

$$q \longleftrightarrow \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ -\alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2 \\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1 \\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}$$

(4) Second regular representation of Q: In a manner similar to that for the first regular representation,

$$q \longleftrightarrow \alpha_0 L_1 + \alpha_1 L_i + \alpha_2 L_j + \alpha_3 L_k$$

and

$$q \longleftrightarrow \alpha_0\, m(L_1) + \alpha_1\, m(L_i) + \alpha_2\, m(L_j) + \alpha_3\, m(L_k)$$

with $L_p$ being defined by $qL_p = pq$ for all $q$ in Q. Thus,

$$m(L_1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$m(L_i) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$$m(L_j) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$m(L_k) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

and, hence,

$$q \longleftrightarrow \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ -\alpha_1 & \alpha_0 & \alpha_3 & -\alpha_2 \\ -\alpha_2 & -\alpha_3 & \alpha_0 & \alpha_1 \\ -\alpha_3 & \alpha_2 & -\alpha_1 & \alpha_0 \end{pmatrix}$$

(5) Rotations: The Euler angles $\psi, \theta, \varphi$ provide the most widely used technique for describing a rotation in $E_3$. Let $0_{xyz}$ denote a right-hand system of rectangular axes fixed in space and let $v$ denote any vector in this system. In theorem 14 it was shown that any rotation of $v$ can be defined by

$$vT_p = pvp^{-1}$$

where $p$ is some fixed nonzero quaternion

$$p = \alpha_0 \cdot 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

This rotation can also be described by three successive Euler angle rotations. The relationship between the quaternion components $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ and the Euler angles $\psi, \theta, \varphi$ is now derived.

Let $R_{\psi,z}$ denote a rotation of $\psi$ about the Z-axis, which rotates the $0_{xyz}$ system into the $0_{x_1y_1z}$ system, and let

$$vR_{\psi,z} = v_1$$

Then, by the corollary of theorem 14, there is a fixed nonzero quaternion $p_1$ such that

$$vR_{\psi,z} = vT_{p_1} = p_1 v p_1^{-1} = v_1$$

where

$$p_1 = \cos\frac{\psi}{2} \cdot 1 - \sin\frac{\psi}{2} k$$

Similarly, let

$$R_{\theta,y_1} : 0_{x_1y_1z} \rightarrow 0_{x'y_1z_1}$$

such that

$$v_1R_{\theta,y_1} = v_2$$

Then there exists a $p_2$ in $Q$ such that

$$v_1R_{\theta,y_1} = v_1T_{p_2} = p_2v_1p_2^{-1} = v_2$$

where

$$p_2 = \cos\frac{\theta}{2}\cdot 1 - \sin\frac{\theta}{2}\,j$$

Finally, let

$$R_{\varphi,x'} : 0_{x'y_1z_1} \rightarrow 0_{x'y'z'}$$

such that

$$v_2R_{\theta,x'} = v'$$

Then, there is a $p_3$ in $Q$ such that

$$v_2R_{\theta,x'} = v_2T_{p_3} = p_3v_2p_3^{-1} = v'$$

where

$$p_3 = \cos\frac{\varphi}{2}\cdot 1 - \sin\frac{\varphi}{2}\,i$$

The total rotation of a vector $v$ in $0_{xyz}$ into $v'$ in $0_{x'y'z'}$ is given by

$$vT_p = pvp^{-1} = v'$$

where $p$ is some fixed nonzero quaternion

$$p = \alpha_0\cdot 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

Since

$$v' = p_3p_2\left(p_1vp_1^{-1}\right)p_2^{-1}p_3^{-1}$$

then

$$p = p_3p_2p_1$$

and, hence

$$p = \left(\cos\frac{\varphi}{2}\cdot 1 - \sin\frac{\varphi}{2}\,i\right)\left(\cos\frac{\theta}{2}\cdot 1 - \sin\frac{\theta}{2}\,j\right)\left(\cos\frac{\psi}{2}\cdot 1 - \sin\frac{\psi}{2}\,k\right)$$

Expanding the right-hand side of this expression gives the following relationships between the quaternion components and Euler angles:

$$\alpha_0 = \cos\frac{\varphi}{2}\cos\frac{\theta}{2}\cos\frac{\psi}{2} + \sin\frac{\varphi}{2}\sin\frac{\theta}{2}\sin\frac{\psi}{2}$$

$$\alpha_1 = \cos\frac{\varphi}{2}\sin\frac{\theta}{2}\sin\frac{\psi}{2} - \sin\frac{\varphi}{2}\cos\frac{\theta}{2}\cos\frac{\psi}{2}$$

$$\alpha_2 = -\cos\frac{\varphi}{2}\sin\frac{\theta}{2}\cos\frac{\psi}{2} - \sin\frac{\varphi}{2}\cos\frac{\theta}{2}\sin\frac{\psi}{2}$$

$$\alpha_3 = -\cos\frac{\varphi}{2}\cos\frac{\theta}{2}\sin\frac{\psi}{2} + \sin\frac{\varphi}{2}\sin\frac{\theta}{2}\cos\frac{\psi}{2}$$

The rotation of $v$ into $v'$ has the following matrix representation in terms of the Euler angles (ref. 15):

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} \cos\psi\cos\theta & \cos\theta\sin\psi & -\sin\theta \\ \cos\psi\sin\theta\sin\varphi - \cos\varphi\sin\psi & \sin\varphi\sin\theta\sin\psi + \cos\psi\cos\varphi & \sin\varphi\cos\theta \\ \cos\varphi\sin\theta\cos\psi + \sin\varphi\sin\psi & \cos\varphi\sin\theta\sin\psi - \sin\varphi\cos\psi & \cos\varphi\cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

Since the Euler transformation is identical to the quaternion transformation, the following additional relationships are easily determined:

$$\psi = \tan^{-1}\left[\frac{2\left(\alpha_1\alpha_2 - \alpha_0\alpha_3\right)}{\left(\alpha_0^2 + \alpha_1^2 - \alpha_2^2 - \alpha_3^2\right)}\right]$$

$$\theta = \sin^{-1}\left[\frac{-2\left(\alpha_1\alpha_3 + \alpha_0\alpha_2\right)}{N(p)}\right]$$

$$\varphi = \tan^{-1}\left[\frac{2\left(\alpha_2\alpha_3 - \alpha_0\alpha_1\right)}{\left(\alpha_0^2 + \alpha_3^2 - \alpha_1^2 - \alpha_2^2\right)}\right]$$

This subject has been discussed in detail in references 15 and 16.

(6) Rate equations (see also refs. 15 and 16): Suppose that the system $0_{x'y'z'}$ is rotating with an angular velocity $\omega$. Let

$$\omega = pi + qj + rk$$

where p, q, and r are the angular velocities about the X', Y', and Z' axes, respectively. The Euler angle rates are expressed as follows (ref. 15):

$$\begin{bmatrix} \dot{\psi} \\ \dot{\theta} \\ \dot{\varphi} \end{bmatrix} = \begin{bmatrix} 0 & \sin\varphi/\cos\theta & \cos\varphi/\cos\theta \\ 0 & \cos\varphi & -\sin\varphi \\ 1 & \sin\varphi \sin\theta/\cos\theta & \cos\varphi \sin\theta/\cos\theta \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

The obvious disadvantage of this system of equations is the singularity existing at

$$\theta = (2n - 1)\frac{\pi}{2} \qquad (n = 1, 2, \ldots)$$

It is now shown that no such problem exists in the corresponding rate equations for the quaternion components. Suppose that the quaternion q is a function of the scalar quantity t – that is,

$$q = q(t) = \omega(t)\cdot 1 + x(t)i + y(t)j + z(t)k$$

Then analogous to the definition of a derivative in the Euclidean vector space of dimension three, define

$$\frac{dq(t)}{dt} = \lim_{\Delta t \to 0} \frac{q(t + \Delta t) - q(t)}{\Delta t}$$

or

$$\frac{d}{dt} q(t) = \frac{d}{dt} \omega(t) \cdot 1 + \frac{d}{dt} x(t)i + \frac{d}{dt} y(t)j + \frac{d}{dt} z(t)k$$

From this expression it follows that

$$\frac{d}{dt}\left(q_1 q_2\right) = \left(\frac{d}{dt} q_1\right) q_2 + q_1 \left(\frac{d}{dt} q_2\right)$$

Now let $T_p$ be the quaternion transformation rotating the vector $v$ in $0_{xyz}$ into $v'$ in $0_{x'y'z'}$ – that is,

$$v' = vT_p = pvp^{-1}$$

where $p$ and $v$ are functions of $t$. Furthermore, let $0_{x'y'z'}$ be rotating with an angular velocity $\omega$ as defined previously. Finally, define the quaternion

$$\lambda = \lambda_0 \cdot 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k$$

by

$$\lambda = \frac{p}{\|p\|} = \frac{p}{+\sqrt{N(p)}}$$

where

$$\lambda_i = \frac{\alpha_i}{\|p\|} \qquad (i = 0, 1, 2, 3)$$

Then

$$v' = vT_p = pvp^{-1} = \lambda v \bar{\lambda}$$

and, also,

$$v = v' T_p^{-1} = p^{-1} v' p = \bar{\lambda} v' \lambda$$

From this relationship, the following matrix representation for $T_p$ is obtained:

$$\begin{bmatrix} \lambda_0^2 + \lambda_1^2 - \lambda_2^2 - \lambda_3^2 & 2(\lambda_1\lambda_2 - \lambda_0\lambda_3) & 2(\lambda_1\lambda_3 + \lambda_0\lambda_2) \\ 2(\lambda_2\lambda_1 + \lambda_3\lambda_0) & \lambda_0^2 + \lambda_2^2 - \lambda_3^2 - \lambda_1^2 & 2(\lambda_2\lambda_3 - \lambda_0\lambda_1) \\ 2(\lambda_3\lambda_1 - \lambda_2\lambda_0) & 2(\lambda_2\lambda_3 + \lambda_0\lambda_1) & \lambda_0^2 + \lambda_3^2 - \lambda_1^2 - \lambda_2^2 \end{bmatrix}$$

From theoretical mechanics (ref. 17, pp. 141-146) is found the following relationship:

$$\left(\frac{dv}{dt}\right)' = \frac{dv'}{dt} + [\omega, v']$$

where $\frac{dv}{dt}$ is a vector in the $0_{xyz}$ or fixed system and $\left(\frac{dv}{dt}\right)'$ denotes the vector $\frac{dv}{dt}$ relative to the moving system $0_{x'y'z'}$. Hence in terms of the quaternion transformation $T_p$, the relationship can be expressed as

$$\left(\frac{dv}{dt}\right)T_p = \left(\frac{dv}{dt}\right)' = \frac{dv'}{dt} + [\omega, v']$$

Now,

$$\left(\frac{dv}{dt}\right)T_p = \lambda\left[\frac{d}{dt}(\bar{\lambda}v'\lambda)\right]\bar{\lambda} = \frac{dv'}{dt} + \lambda\left(\frac{d}{dt}\bar{\lambda}\right)v' + v'\left(\frac{d}{dt}\lambda\right)\bar{\lambda}$$

Since $\lambda\bar{\lambda} = 1$,

$$\left(\frac{dv}{dt}\right)T_p = \frac{dv'}{dt} - \left(\frac{d}{dt}\lambda\right)\bar{\lambda}v' + v'\left(\frac{d}{dt}\lambda\right)\bar{\lambda}$$

Thus,

$$[\omega, v'] = v'\left(\frac{d}{dt}\lambda\right)\bar{\lambda} - \left(\frac{d}{dt}\lambda\right)\bar{\lambda}v'$$

Note that for any $\lambda$ in Q

$$\left(\frac{d}{dt}\lambda\right)\bar{\lambda} = r^* + v^*$$

where $r^*$ is in I and $v^*$ is in $E_3$. Then, from (c) of property (1) is found

$$[\omega, v'] = -2[v^*, v']$$

or

$$\left[\omega + 2v^*, v'\right] = 0$$

Since this expression is valid for all $v'$ in $E_3$ and since the vector cross product is nondegenerate,

$$\omega = -2v^*$$

Finally,

$$v^* = \frac{1}{2}\left[\left(\frac{d}{dt}\lambda\right)\bar{\lambda} - \overline{\left(\frac{d}{dt}\lambda\right)\bar{\lambda}}\right] = \frac{1}{2}\left[\left(\frac{d}{dt}\lambda\right)\bar{\lambda} - \lambda\left(\frac{d}{dt}\bar{\lambda}\right)\right]$$

Again, since $\lambda\bar{\lambda} = 1$,

$$v^* = \left(\frac{d}{dt}\lambda\right)\bar{\lambda}$$

Thus,

$$\omega = -2\left(\frac{d}{dt}\lambda\right)\bar{\lambda}$$

or

$$\frac{d}{dt}\lambda = -\frac{1}{2}\omega\lambda$$

Expanding this expression gives the following matrix representation:

$$\begin{bmatrix} \dot{\lambda}_0 \\ \dot{\lambda}_1 \\ \dot{\lambda}_2 \\ \dot{\lambda}_3 \end{bmatrix} = -\frac{1}{2}\begin{bmatrix} 0 & -p & -q & -r \\ p & 0 & -r & q \\ q & r & 0 & -p \\ r & -q & p & 0 \end{bmatrix}\begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix}$$

Equivalently,

$$\begin{bmatrix} \dot{\lambda}_0 \\ \dot{\lambda}_1 \\ \dot{\lambda}_2 \\ \dot{\lambda}_3 \end{bmatrix} = -\frac{1}{2} \begin{bmatrix} -\lambda_1 & -\lambda_2 & -\lambda_3 \\ \lambda_0 & \lambda_3 & -\lambda_2 \\ -\lambda_3 & \lambda_0 & \lambda_1 \\ \lambda_2 & -\lambda_1 & \lambda_0 \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

where

$$\dot{\lambda}_i = \frac{d}{dt} \lambda_i \qquad (i = 0, 1, 2, 3)$$

Note that the substitution

$$\lambda = \frac{p}{+\sqrt{N(p)}}$$

is equivalent to using $vT_p = pvp^{-1}$ and applying the constraint

$$p\bar{p} = N(p) = 1$$

Normally, direction cosines are used to avoid the problem of gimbal lock. However, this involves the three Euler angle differential equations being replaced by six direction cosine differential equations with three algebra equations and three constraints. On the other hand, representing rigid-body rotations with quaternions involves only four differential equations with one constraint.

## RÉSUMÉ

Some characterizations and properties of linear algebras over the field of real numbers are as follows:

1. Every real algebra is a normed algebra and every real absolute valued algebra is a division algebra.

2. Given a real absolute valued algebra without associativity of multiplication, one is not assured of the existence of an identity element. However, multiplication can be redefined in such a way that the resultant algebra is an absolute valued algebra with identity.

3. The algebra of real quaternions is a unique associative division algebra which is isomorphic and anti-isomorphic to algebras of real $n \times n$ matrices.

4. The collection of all automorphisms on the algebra of real quaternions defines the group of all rotations on the real Euclidean vector space of dimension three. The advantage of representing rigid-body rotations with quaternions is in the elimination of the gimbal lock problem encountered when using Euler angles.

Langley Research Center,
National Aeronautics and Space Administration,
Langley Station, Hampton, Va., September 14, 1966,
125-23-02-04-23.

## REFERENCES


1. Albert, A. A.: Absolute Valued Real Algebras. Ann. Math., Second ser., vol. 48, no. 2, Apr. 1947, pp. 495-501.

2. Dickson, L. E.: On Quaternions and Their Generalization and the History of the Eight Square Theorem. Ann. Math., Second ser., vol. 20, 1918-1919, pp. 155-171.

3. Kleinfeld, Erwin: A Characterization of the Cayley Numbers. Studies in Modern Algebra, Vol. 2 of Studies in Mathematics, A. A. Albert, ed., Math. Assoc. Am., c.1963, pp. 126-143.

4. Curtis, Charles W.: The Four and Eight Square Problem and Division Algebras. Studies in Modern Algebra, Vol. 2 of Studies in Mathematics, A. A. Albert, ed., Math. Assoc. Am., c.1963, pp. 100-125.

5. Jacobson, N.: Composition Algebras and Their Automorphisms. Rend. Circ. Mat. Palermo, ser. 2, vol. 7, 1958, pp. 55-80.

6. Herstein, I. N.: Topics in Algebra. Blaisdell Pub. Co., c.1964.

7. Bruck, R. H.; and Kleinfeld, Erwin: The Structure of Alternative Division Rings. Proc. Am. Math. Soc., vol. 2, no. 6, Dec. 1951, pp. 878-890.

8. McCoy, Neal H.: Rings and Ideals. Carus Math. Monographs No. 8, Math. Assoc. Am., c.1948.

9. Dickson, L. E.: Linear Algebras. Hafner Pub. Co.

10. Birkhoff, Garrett; and MacLane, Saunders: A Survey of Modern Algebra. The Revised ed., The Macmillan Co., c.1953.

11. MacDuffee, Cyrus Colton: An Introduction to Abstract Algebra. John Wiley and Sons, Inc., 1940.

12. Olmsted, John M. H.: Real Variables. Appleton-Century-Crofts, Inc., c.1959.

13. Whittaker, E. T.: A Treatise on the Analytical Dynamics of Particles and Rigid Bodies. Fourth ed., Cambridge Univ. Press, 1960.

14. Brand, Louis: Vector and Tensor Analysis. John Wiley & Sons, Inc., c.1947.

15. Niemz, Werner: Anwendung der Quaternionen auf die allgemeinen Bewegungsgleichungen der Flugmechanik. Z. Flugwissenschaften. Jahrg. 11, Heft 9, 1963, pp. 368-372.

16. Surber, T. E.: On the Use of Quaternions to Describe the Angular Orientation of Space Vehicles. J. Aerospace Sci. (Readers' Forum), vol. 28, no. 1, Jan. 1961, pp. 79-80.

17. Corben, H. C.; and Stehle, Philip: Classical Mechanics, 2nd ed., John Wiley & Sons, Inc., c.1960.

*"The aeronautical and space activities of the United States shall be conducted so as to contribute . . . to the expansion of human knowledge of phenomena in the atmosphere and space. The Administration shall provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."*

—NATIONAL AERONAUTICS AND SPACE ACT OF 1958

# NASA SCIENTIFIC AND TECHNICAL PUBLICATIONS

TECHNICAL REPORTS: Scientific and technical information considered important, complete, and a lasting contribution to existing knowledge.

TECHNICAL NOTES: Information less broad in scope but nevertheless of importance as a contribution to existing knowledge.

TECHNICAL MEMORANDUMS: Information receiving limited distribution because of preliminary data, security classification, or other reasons.

CONTRACTOR REPORTS: Technical information generated in connection with a NASA contract or grant and released under NASA auspices.

TECHNICAL TRANSLATIONS: Information published in a foreign language considered to merit NASA distribution in English.

TECHNICAL REPRINTS: Information derived from NASA activities and initially published in the form of journal articles.

SPECIAL PUBLICATIONS: Information derived from or of value to NASA activities but not necessarily reporting the results of individual NASA-programmed scientific efforts. Publications include conference proceedings, monographs, data compilations, handbooks, sourcebooks, and special bibliographies.

***Details on the availability of these publications may be obtained from:***


**SCIENTIFIC AND TECHNICAL INFORMATION DIVISION**

**NATIONAL AERONAUTICS AND SPACE ADMINISTRATION**

**Washington, D.C. 20546**